

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-269524

(P2002-269524A)

(43) 公開日 平成14年9月20日 (2002.9.20)

(51) Int.Cl.⁷

識別記号

F I

テーマコード(参考)

G 0 6 K 19/077

B 4 2 D 15/10

G 0 6 K 19/073

5 2 1

B 4 2 D 15/10

G 0 6 K 19/00

5 2 1

2 C 0 0 5

K 5 B 0 3 5

P

審査請求 未請求 請求項の数 3 O L (全 7 頁)

(21) 出願番号 特願2001-67248(P2001-67248)

(22) 出願日 平成13年3月9日(2001.3.9)

(71) 出願人 000000295

沖電気工業株式会社

東京都港区虎ノ門1丁目7番12号

(72) 発明者 宇佐見 慎一

東京都港区虎ノ門1丁目7番12号 沖電気

工業株式会社内

(74) 代理人 100086807

弁理士 柿本 恭成

Fターム(参考) 2C005 MA03 MA27 MA34 MB01 PA27

QC04 RA12 SA03

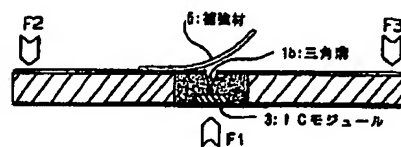
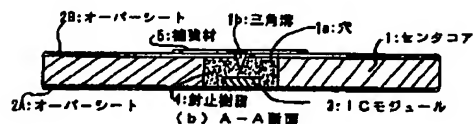
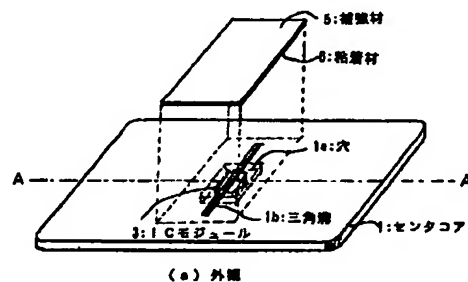
5B035 AA13 BA03 BB09 CA01 CA38

(54) 【発明の名称】 ICカード

(57) 【要約】

【課題】 廃棄時に容易にセキュリティを確保できる ICカードを提供する。

【解決手段】 プラスチック製のセンタコア1に空けられた穴1aの内部に、ICモジュール3が封止樹脂4で埋め込まれたICカードにおいて、このICモジュール3の埋め込み箇所に対応するカード表面に、所定の深さの三角溝1bを設け、この三角溝1bを覆うように補強材5を粘着材6で貼り付ける。これにより、ICカードは通常の強度を保つことができる。廃棄時には、補強材5を剥がし、三角溝1bの下側から指等で力F1を加えると共に、カードの両端に逆方向の力F2、F3を加える。これにより、三角溝1bの箇所でICモジュール3が確実に破壊され、このICモジュール3に記憶された情報を読み出すことができなくなる。



(c) 破壊方法

本発明の第1の実施形態のICカード

【特許請求の範囲】

【請求項1】 プラスチック製のカードにICモジュールを埋め込んで形成されたICカードにおいて、前記ICモジュールの埋め込み箇所に対応するカード表面に所定の深さの溝を設けると共に、該溝を覆うように該カード表面に補強材を非硬化性の粘着材で貼り付けたことを特徴とするICカード。

【請求項2】 入力された情報を予め組み込まれたプログラムに従って処理する機能部と、前記機能部の処理結果を格納する不揮発性の記憶部と、導電性塗料で形成された固有の配線パターンに従って暗号キーを発生するコード発生部と、前記機能部から出力された処理結果のデータを前記暗号キーに従って暗号化して前記記憶部に書き込む共に、該記憶部から読み出されたデータを該暗号キーに従って復号化して該機能部に与える暗号部と、前記機能部、記憶部、コード発生部及び暗号部を埋め込むと共に、該コード発生部の配線パターンを露出させる窓部を有するプラスチック製のカードと、前記カードの窓部を覆う蓋とを、備えたことを特徴とするICカード。

【請求項3】 導電性塗料で形成された固有の配線パターンに従って固有コードを発生するコード発生部と、予め設定された識別コードと前記固有コードが一致したときに動作許可信号を出力する一致検出部と、前記動作許可信号が与えられたときに、入力された情報を予め組み込まれたプログラムに従って処理する機能部と、前記コード発生部、一致検出部及び機能部を埋め込むと共に、該コード発生部の配線パターンを露出させる窓部を有するプラスチック製のカードと、前記カードの窓部を覆う蓋とを、備えたことを特徴とするICカード。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】 本発明は、IC（集積回路）カード、特に廃棄時に記憶情報を読めなくしてセキュリティを確保する技術に関するものである。

【0002】

【従来の技術】 ICカードに個人情報等の機密性の高い情報を記録して利用する場合、そのカードが不要になったときにそのまま廃棄すると、そこに記録されている情報が漏洩して問題となるおそれがある。そのため、ICカードの廃棄時には、そこに記録されている情報を確実に読み出せなくする必要がある。

【0003】 従来、ICカードに記録された情報を読み出せなくする方法としては、専用の装置によって情報を電氣的に消去する方法、専用の機械によってICカードを物理的に破壊する方法、使用者がはさみ等の一般的な道具で破壊する方法等が採られていた。

【0004】

【発明が解決しようとする課題】 しかしながら、従来のように、何らかの装置、機械または道具が必要であると、使用者が何時でも処置を行えるとは限らないので、使用者の怠慢等により廃棄時の適切な処置が徹底されないおそれが多い。

【0005】 また、専用の装置で情報を消去した場合でも、確実に消去されたか否かを目視で確認できないので、廃棄時に感情的に不安が残る。また、はさみ等の道具で破壊した場合でも、ICチップ部分が破壊されずにそのまま残っていると、情報が漏洩するおそれがある。

【0006】 本発明は、前記従来技術が持っていた課題を解決し、廃棄時に道具等を使用せずに、容易に記録情報を読み出せなくしてセキュリティを確保できるICカードを提供するものである。

【0007】

【課題を解決するための手段】 前記課題を解決するために、本発明の内の第1の発明は、プラスチック製のカードにICモジュールを埋め込んで形成されたICカードにおいて、前記ICモジュールの埋め込み箇所に対応するカード表面に所定の深さの溝を設けると共に、該溝を覆うように該カード表面に補強材を非硬化性の粘着材で貼り付けている。

【0008】 第1の発明によれば、以上のようにICカードを構成したので、このICカードを廃棄する場合、カード表面の補強材を剥がし、このカード表面に設けられた溝の部分で折り曲げれば良い。これにより、溝の部分において埋め込まれたICモジュールが破壊され、このICモジュール内に格納された情報を読み出すことができなくなり、セキュリティを確保することができる。

【0009】 第2の発明は、ICカードにおいて、入力された情報を予め組み込まれたプログラムに従って処理する機能部と、前記機能部の処理結果を格納する不揮発性の記憶部と、導電性塗料で形成された固有の配線パターンに従って暗号キーを発生するコード発生部と、前記機能部から出力された処理結果のデータを前記暗号キーに従って暗号化して前記記憶部に書き込むと共に、該記憶部から読み出されたデータを該暗号キーに従って復号化して該機能部に与える暗号部と、前記機能部、記憶部、コード発生部及び暗号部を埋め込むと共に、該コード発生部の配線パターンを露出させる窓部を有するプラスチック製のカードと、前記カードの窓部を覆う蓋とを備えている。

【0010】 第2の発明によれば、このICカードを廃棄する場合、窓部の蓋を取り外して、コード発生部の導電性塗料による固有の配線パターンを削り取れば良い。これにより、暗号部に与えられる暗号キーが変更され、変更前の暗号キーで暗号化されて記憶部に書き込まれているデータを正しく読み出すことができなくなる。

【0011】 第3の発明は、ICカードにおいて、導電

性塗料で形成された固有の配線パターンに従って固有コードを発生するコード発生部と、予め設定された識別コードと前記固有コードが一致したときに動作許可信号を出力する一致検出部と、前記動作許可信号が与えられたときに、入力された情報を予め組み込まれたプログラムに従って処理する機能部と、前記コード発生部、一致検出部及び機能部を埋め込むと共に、該コード発生部の配線パターンを露出させる窓部を有するプラスチック製のカードと、前記カードの窓部を覆う蓋とを備えている。

【0012】第3の発明によれば、このICカードを廃棄する場合、窓部の蓋を取り外して、コード発生部の導電性塗料による固有の配線パターンを削り取れば良い。これにより、一致検出部に与えられる固有コードが変更され、予め設定されている識別コードに一致しなくなるので、機能部の動作が不可能になり、他人に使用されるおそれなくなる。

【0013】

【発明の実施の形態】（第1の実施形態）図1(a)～(c)は、本発明の第1の実施形態を示すICカードの概略の構成図であり、同図(a)は外観を示す組立図、同図(b)は同図(a)におけるA-A断面図、及び同図(c)は廃棄方法を示す説明図である。

【0014】このICカードは、図1(a)、(b)に示すように、縦54mm、横86mm、厚さ0.5mm程度の、硬質塩化ビニール等のプラスチックを材料とするセンタコア（中心部材）1の両面を、同様のプラスチックによるオーバーシート2A、2Bでサンドイッチ状に挟んで、一体化した構造となっている。標準的なICカードの全体の厚さは、0.76mm程度である。

【0015】センタコア1の所定の位置には、ICモジュール3を収納するための穴1aが設けられており、オーバーシート2AにこのICモジュール3が接着されている。穴1aには、ICモジュール3を保護すると共にカードの強度を維持するために、封止樹脂4が充填されている。

【0016】更に、ICカードの中央部の表面には、ICモジュール3の上部を通るように、縦方向に直線状の三角溝1bが設けられている。三角溝1bの深さは、オーバーシート2Bを越えて封止樹脂4及びセンタコア1の一部まで達するが、ICモジュール3には届かない程度に形成されている。三角溝1bの表面には、硬質塩化ビニール板等の補強材5が非硬化性の粘着材6で貼り付けられている。

【0017】このようなICカードは、例えば、次のような工程で製造される。まず、ICモジュール3を収納するための穴1aを空けたセンタコア1の一方の面に、オーバーシート2Aを熱接着し、この穴1aの底部にICモジュール3を接着剤で固定した後、その上に封止樹脂4を注入して硬化させる。更に、センタコア1の他の面にオーバーシート2Bを熱接着する。ここまでは、従

来通りのICカードの製造工程である。

【0018】次に、カッター等を使用して、ICカードの縦方向に一定の長さで深さを有する三角溝1bを形成する。このとき、三角溝1bは、オーバーシート2Bの上から、ICモジュール3の上部を通り、このICモジュール3に達しないような深さに形成する。

【0019】更に、三角溝1bを覆うように、オーバーシート2Bの表面に補強材5を非硬化性の粘着材6で貼り付ける。これによって、本実施形態のICカードが完成する。

【0020】このようなICカードは、オーバーシート2Bの表面に補強材5が貼り付けられた状態で使用される。これにより、三角溝1bによる強度的な弱点箇所が補強材5で補強され、通常の強度を保つことができる。

【0021】一方、このICカードを廃棄する場合には、図1(c)に示すように、オーバーシート2Bの表面から補強材5を剥がし、三角溝1bの下側から指等で上向きに力F1を加えると共に、ICカードの両端に下向きの力F2、F3を加える。これにより、ICカードは三角溝1bの箇所では折り曲げられ、ICモジュール3が完全に破壊される。

【0022】以上のように、この第1の実施形態のICカードは、ICモジュール3の上部に折り曲げ用の三角溝1bを有するので、道具を使用せずにICモジュール3を完全に破壊することができる。従って、廃棄時に記録情報を読み出せなくしてセキュリティを確保できる。また、ICモジュール3が破壊されたことを、目視または手触り等で確認することができるので、安心してICカードを廃棄することができるという利点がある。

【0023】（第2の実施形態）図2(a)～(c)は、本発明の第2の実施形態を示すICカードの概略の構成図であり、同図(a)は外観を示す組立図、同図(b)は同図(a)におけるB-B断面図、及び同図(c)はコード発生部の平面図である。

【0024】このICカードは、図2(a)、(b)に示すように、縦54mm、横86mm、厚さ0.76mm程度の、硬質塩化ビニール等のプラスチックを材料とするICカード本体10の内部に、コード発生部20、信号線群30及びICモジュール40を埋め込んだ構造となっている。コード発生部20の上部には、窓部11が開口され、この窓部11が蓋12で塞がれている。蓋12の周囲は、非硬化性の粘着材で封止され、使用中に蓋12が外れたり、隙間からゴミや湿気等が侵入しないようになっている。

【0025】コード発生部20は図2(c)に示すように、基板21上に、例えば電源電位VDDに接続される1つのノード22と、コード出力用の複数のノード23（但し、 $i=1\sim n$ 、例えば $n=100$ ）を設けたものである。ノード23_iの内の幾つかとノード22の間は、導電性塗料を塗布して形成された固有の配線パター

ン24によって、ランダムに接続されている。

【0026】図3は、図2のICカードの回路図である。このICカードは、前述のコード発生部20、ICモジュール40及びこれらの間を接続する信号線群30を有している。コード発生部20のノード22は、電源電位VDDに接続され、各ノード23は、それぞれ信号線31を介して、ICモジュール40に接続されている。

【0027】ICモジュール40は、各信号線31に対応するプルダウン用の抵抗41とバッファ42、暗号部43、データバス44a、44b、機能部45、記憶部46及びアドレスバス47を有している。

【0028】バッファ42の出力側は、暗号部43に接続されている。暗号部43は、バッファ42から与えられる信号を暗号キーとして、データバス44a上のデータを暗号化してデータバス44bに出力すると共に、データバス44b上のデータを復号化してデータバス44aに出力するものである。

【0029】データバス44aには、機能部45が接続されている。機能部45は、CPU（中央処理装置）、ROM（読出専用メモリ）、RAM（随時読み書き可能なメモリ）及び入出力部等で構成され、入力部から入力された情報を、ROMに組み込まれたプログラムに従って処理するものである。

【0030】データバス44bには、記憶部46が接続されている。記憶部46は、EEPROM（電氣的に書き換え可能な不揮発性メモリ）等で構成され、機能部45の処理結果である個人情報等のセキュリティを必要とする情報を格納するものである。

【0031】アドレスバス47は、機能部45から記憶部46に対して、読み書きのアドレスを指定するためのものである。

【0032】次に、動作を説明する。コード発生部20のノード23は、導電性塗料で形成された固有の配線パターン24でランダムにノード22に接続されているので、これらの各ノード23の電位は配線パターン24の形状によって異なる。即ち、配線パターン24で接続されているノード23は、電源電位VDDとなり、配線パターン24で接続されていないノード23には、電圧が出力されない。

【0033】各ノード23の電位は、それぞれ信号線31を介して、ICモジュール40内のバッファ42の入力側に導かれる。各バッファ42の入力側には、プルダウン用の抵抗41が接続されているので、配線パターン24で接続されていないノード23に対応する信号線31は、接地電位GNDとなる。また、配線パターン24に接続されたノード23に対応する信号線31は、電源電位VDDとなる。これらの信号線31の電位は、それぞれバッファ42を介して、暗号キーとして暗号部43に与えられる。

【0034】ここで、機能部45から記憶部46に対して書き込み動作が行われると、この機能部45からアドレスバス47を介して書き込み対象のアドレスが指定され、データバス44a上に書き込むデータが出力される。データバス44aに出力されたデータは、暗号部43によって暗号化されてデータバス44bに出力される。そして、暗号化されたデータが記憶部46に書き込まれる。

【0035】次に、機能部45から記憶部46に対して読み出し動作が行われると、この機能部45からアドレスバス47を介して読み出し対象のアドレスが指定される。これにより、記憶部46に格納されている暗号化されたデータが読み出され、データバス44b上に出力される。データバス44bに出力されたデータは、暗号部43によって復号化されてデータバス44aに出力される。そして、復号化されたデータが、機能部45に読み取られる。暗号部43に与えられる暗号キーは、コード発生部20の配線パターン24が変わらない限り変化しないので、機能部45では書き込んだ通りのデータを読み出すことができる。

【0036】一方、このICカードを廃棄する場合には、図2(a)に示すように蓋12を外し、窓部11の内側にあるコード発生部20の表面の配線パターン（導電性塗料）24を、爪等で削り取る。これにより、配線パターン24が変更され、暗号部43に与えられる暗号キーが変化する。このため、機能部45から記憶部46に対して読み出し動作を行おうとすると、暗号キーが書き込み時から変化しているため、データを正しく読み出すことができない。

【0037】以上のように、この第2の実施形態のICカードは、導電性塗料による固有の配線パターン24で暗号キーを発生するコード発生部20を有すると共に、ICカード本体10に設けた蓋12を外すことによって、このコード発生部20の配線パターン24を簡単に削り取ることができるようになっている。従って、廃棄時に容易に暗号キーを変え、記憶部45の記録情報を読み出せなくしてセキュリティを確保することができる。

【0038】また、コード発生部20の配線パターン24を削り取ったことを、目視で確認することができるので、安心してICカードを廃棄することができるという利点がある。更に、ICカード自体を破壊した訳ではないので、記憶部46の記憶内容をすべて消去し、コード発生部20の配線パターン24を塗り替えば、再利用することができるという利点がある。

【0039】（第3の実施形態）図4は、本発明の第3の実施形態を示すICカードの回路図であり、図3中の要素と共通の要素には共通の符号が付されている。

【0040】このICカードでは、図3中のICモジュール40に代えて、回路構成の異なるICモジュール40Aを用いている。なお、本実施形態のICカードの外

観は、図2(a)～(c)に示した第2の実施形態のICカードと同様である。

【0041】ICモジュール40Aは、コード発生部20の各ノード23_iに接続された信号線31_iをプルダウンするための抵抗41_i、コード設定部48、一致検出部49、機能部45A及び記憶部46を有している。

【0042】コード設定部48は、このICカードを特定するためのnビットの識別コードを予め設定するもので、例えば、n個のトランジスタの内、ゲートに選択的にイオンを注入してオン状態にしたトランジスタと、イオンを注入しないオフ状態のトランジスタの組み合わせによるマスクROMで構成されている。

【0043】一致検出部49は、コード発生部20の各ノード23_iから信号線31_iを介して与えられる固有コードと、コード設定部48に設定された識別コードを比較して、これらが一致したときに動作許可信号ENを出力するものである。一致検出部49は、コード発生部20とコード設定部48から与えられる対応する信号同士を比較するn個のXNOR（排他的否定論理和ゲート）と、これらのXNORの出力信号の論理積を動作許可信号ENとして出力するAND（論理積ゲート）とで構成されている。一致検出部49の出力側は、機能部45Aのイネーブル端子に接続されている。

【0044】機能部45Aは、CPU、ROM、RAM、入出力部等で構成され、イネーブル端子に動作許可信号ENが与えられたときに、入力部から入力された情報をROMに組み込まれたプログラムに従って処理するものである。機能部45Aには、システムバスを介してEEPROM等の記憶部46が接続されている。

【0045】このようなICカードは、製造時に、ICモジュール40Aのコード設定部48にカード毎に固有の識別コードを設定し、コード発生部20にはこの識別コードと同じ固有コードを発生させるための配線パターン24を導電性塗料で形成する。

【0046】このようにして製造されたICカードでは、コード発生部20で発生された固有コードと、コード設定部48に設定された識別コードが同一であるので、一致検出部49から機能部45Aに対して動作許可信号ENが出力される。これにより、機能部45Aによって所定の処理が行われ、処理結果の情報が記憶部46に格納される。

【0047】一方、このICカードを廃棄する場合には、図2(a)に示すように蓋12を外し、窓部11の内側にあるコード発生部20の表面を露出させる。そして、導電性塗料による配線パターン24を、爪等で削り取る。これにより、配線パターン24が変更され、一致検出部49に与えられる固有コードが変化する。このため、一致検出部49から機能部45Aに対する動作許可信号ENが停止し、ICカードの使用が不可能になる。

【0048】以上のように、この第3の実施形態のIC

カードは、導電性塗料による固有の配線パターン24で、予め設定された識別コードと同じ固有コードを発生するコード発生部20を有すると共に、ICカード本体10に設けた蓋12を取ることによって、このコード発生部20の配線パターン24を簡単に削り取ることができるようにになっている。従って、廃棄時に容易に固有コードを変え、ICカード自体を使用不可能な状態にすることができ、記憶部46の記録情報を読み出せなくしてセキュリティを確保することができる。

【0049】また、コード発生部20の配線パターン24を削り取ったことを、目視で確認することができるので、安心してICカードを廃棄することができるという利点がある。

【0050】なお、本発明は、上記実施形態に限定されず、種々の変形が可能である。この変形例としては、例えば、次のようなものがある。

【0051】(a) 図1のICカードでは、廃棄時にICモジュール3を確実にかつ容易に破壊するために、三角溝1bを設けているが、矩形や半円形の溝でも良い。

【0052】(b) 図1中の補強材5は、ICカード表面の一部にだけ貼り付けているが、このICカード全面に貼り付けても良い。これにより、表面が平らに仕上がり、操作性及び体裁が良くなる。

【0053】(c) 図2のICカードでは、製造時に、予め固有の配線パターン24を形成して個々の暗号キーを発生させるようにしてから、ICカード本体10に埋め込み、更に窓部11を蓋12で閉じて完成したICカードとしている。しかし、製造時に、コード発生部20のノード22をすべてのノード23_iに接続する配線パターン24を形成しておき、ユーザが使用開始の直前に配線パターン24の一部を削って固有の暗号キーを発生させるようにしても良い。これにより、廃棄後に暗号キーを知ることが一層困難になり、セキュリティを保護することができる。この場合、製造時には、窓部11に蓋12を仮り止めしておき、ユーザが固有の暗号キーを設定した時点で、蓋12を固定するようにする必要がある。

【0054】(d) 図3及び図4において、コード発生部20のノード22を電源電位VDDに接続しているが、このノード22を接地電位GNDに接続しても良い。その場合、抵抗41_iはプルアップ抵抗として一端を電源電位VDDに接続する必要がある。

【0055】

【発明の効果】以上詳細に説明したように、第1の発明によれば、ICモジュールの埋め込み箇所カード表面に溝を設け、この溝を覆うように補強用のプラスチック板を粘着材で貼り付けている。従って、プラスチック板により通常の使用状態での強度が保たれ、廃棄時には、プラスチック板を剥がして溝の部分でカード本体を折り曲げるにより、ICモジュールを確実に破壊するこ

とができる。これにより、廃棄時のセキュリティを容易に確保することができる。

【0056】第2の発明によれば、導電性塗料による配線パターンで暗号キーを発生するコード発生部と、この暗号キーを使用して機能部と記憶部の間のデータを暗号化する暗号部を有している。従って、廃棄時に配線パターンを削り取れば暗号キーが変更され、記憶部に格納されたデータを正しく読み出すことができなくなる。これにより、廃棄時のセキュリティを容易に確保することができる。

【0057】第3の発明によれば、導電性塗料による配線パターンで固有コードを発生するコード発生部と、この固有コードが予め設定された識別コードと一致したときに動作許可信号を出力する一致検出部を有している。従って、廃棄時に配線パターンを削り取れば固有コードが変更され、動作許可信号が停止して機能部の処理が不可能になる。これにより、廃棄時のセキュリティを容易に確保することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態を示すICカードの概略の構成図である。

【図2】本発明の第2の実施形態を示すICカードの概略の構成図である。

【図3】図2のICカードの回路図である。

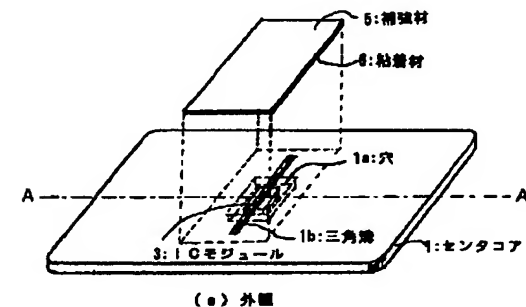
【図4】本発明の第3の実施形態を示すICカードの回*

* 路図である。

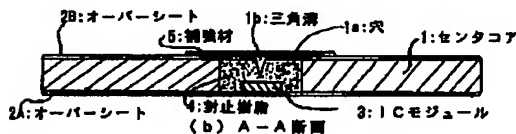
【符号の説明】

- 1 センタコア
- 2A, 2B オーバーシート
- 3, 40, 40A ICモジュール
- 4 封止樹脂
- 5 補強材
- 6 粘着材
- 10 ICカード本体
- 11 窓部
- 12 蓋
- 20 コード発生部
- 22, 23 ノード
- 24 配線パターン
- 31 信号線
- 41 抵抗
- 42 バッファ
- 43 暗号部
- 44a, 44b データバス
- 45, 45A 機能部
- 46 記憶部
- 47 アドレスバス
- 48 コード設定部
- 49 一致検出部

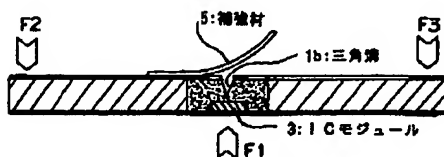
【図1】



(a) 外観



(b) A-A断面



(c) 製造方法

本発明の第1の実施形態のICカード

【図3】

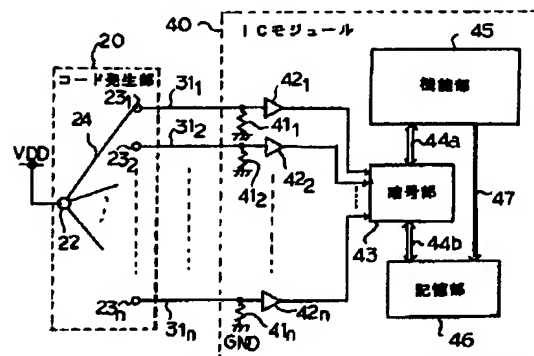
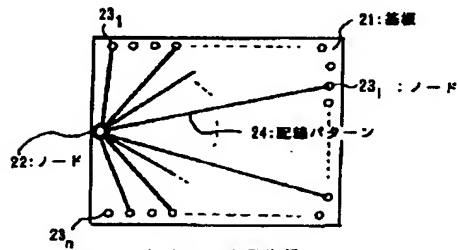
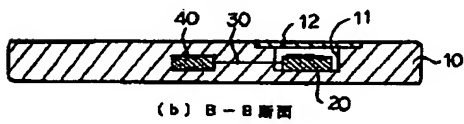
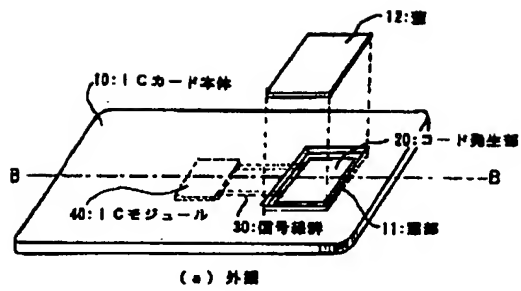


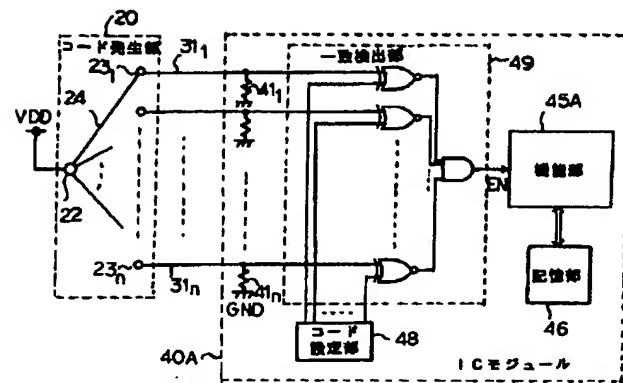
図2のICカードの回路

【図2】



本発明の第2の実施形態のICカード

【図4】



本発明の第3の実施形態のICカードの回路

THIS PAGE BLANK (USPTO)